

HEADQUARTERS
UNITED STATES EUROPEAN COMMAND
APO AE 09128

05 FEB 1996

DIRECTIVE
NUMBER 25-11

SECURITY

Travel Briefing Requirements for Designated Personnel

1. Purpose. To prescribe policies and procedures requiring security briefings for all U.S. personnel possessing a security clearance and/or those indoctrinated for access to Sensitive Compartmented Information (SCI).

2. Applicability. This Directive applies to all HQ USEUCOM Directorates/Staff offices and Activities internal and external to the Headquarters, not including component commands.

3. Internal Control Systems. This Directive contains internal control provisions and is subject to requirements of the internal management control program. For HQ USEUCOM and subordinate joint activities, the applicable internal control directive is ED 50-8, Internal Management Control Program.

4. Suggested Improvements. The proponent for this directive is the Intelligence Directorate, Special Security Office. Suggested improvements should be forward to HQ USEUCOM, Attn: ECJ2-SSO, Unit 30400, Box 1000, APO AE 09128.

5. References.

a. DoD 5200.2-R, Personnel Security Program, January 1987 (U).

b. DoD S-5105.21-M-1, Sensitive Compartmented Information Administrative Security Manual, March 1995 (U).
8

c. Director of Central Intelligence Directive (DCID) 1/20, Security Policy Concerning Travel and Assignment of Personnel with Access to Sensitive Compartmented Information

(SCI), 29 December 1991 (U).

d. CJCS Instruction 3231.01, Safeguarding the SIOP, dated 30 Nov 93 (U).

6. Explanation of Terms.

a. Defensive Security Briefings. Formal advisories that alert traveling personnel to the potential for harassment, exploitation, provocation, capture, or entrapment. These briefings, based on actual experience, include information on courses of action helpful in mitigating adverse security and personnel consequences, and advice of passive and active measures that personnel should take to avoid becoming targets or inadvertent victims as a consequence of hazardous travel.

b. Official Travel. Travel performed at the direction of the U.S. Government.

c. Unofficial Travel. Travel undertaken by an individual without official fiscal, or other obligations on the part of the U.S. Government.

d. Class I Personnel. U.S. military, civilian and DoD contractor personnel indoctrinated for any level of access to Sensitive Compartmented Information (SCI).

e. Class II Personnel. Persons other than those designated as Class I who possess a DoD security clearance and are considered by their directors or activity heads as vulnerable because of their broad knowledge of critical defense matters. Generally, this includes persons who are engaged in working with war plans, cover and deception, plans and

This Directive supersedes SM 25-3, dated 23 Jan 87.

05 FEB 1996

polices, restricted data, Critical Nuclear Weapons Design Information (CNWDI), the Single Integrated Operational Plan -Extremely Sensitive Information (SIOP-ESI), Special Contingency Plans, similarly critical information or activities, and specifically those possessing a U.S. Top Secret clearance. This applies to U.S. military, civilian, and DoD contractor personnel.

f. Hazardous Travel. Travel to, through, or within countries which pose a threat to Class I and II personnel. Hazardous travel includes:

(1) Travel to, through, or within:

(a) Combat zones

(b) Countries identified as medium or high risk by the States Department.

(c) Areas in which the threat to U.S. personnel from foreign intelligence services, terrorist or narcotics groups, or indigenous groups active in promoting insurgency, war, or civil physical safety and security of personnel and sensitive information cannot be reasonably insured.

(2) Travel or visits to diplomatic or trade mission of counties identified as medium or high risk by the State Department.

(3) Travel on transportation carriers owned or controlled by a country identified as medium or high risk by the State Department.

7. Responsibilities.

a. The EJC2 Special Security Office (SSO) will:

(1) Maintain a master Roster of all Class I Personnel.

(2) Distribute State Department and other appropriate Agency warnings to Directorate or Activity SCI Billet Managers, or subordinate SSOs and representatives.

b. The HQ USEUCOM Collateral Personnel Security Office will:

(1) Maintain a master file of all Class II Personnel.

(2) Distribute State Department and other appropriate Agency warnings to Directorate or Activity Security Managers, as needed.

c. At HQ USEUCOM, Unit/Activity SCI Billet Managers will process the HQ USEUCOM Form 25-11A-R and arrange for Defensive Security Briefings for Class I Personnel under their jurisdiction. Locations outside of HQ USEUCOM will coordinate directly with their managing SSO.

d. HQ USEUCOM Directorate/Unit Security Managers, or their designated appointee, will:

(1) Process the HQ USEUCOM Form 25-11B-R and arrange for Defensive Security Briefing for Class II Personnel under their Jurisdiction.

(2) Ensure that those personnel with access to other programs having travel restrictions or requiring special briefings/debriefings are referred to the appropriate program manager or administrator. This includes personnel in both Categories I and II. Examples include, but are not limited to, those personnel read-on to Special Access Programs (SAPs) and/or access to the Single Integrated Operational Plan - Extremely Sensitive Information - and Critical Nuclear Weapons Design Information.

(3) Schedule newly arrive personnel for a "Subversion and Espionage Directed Against Armed Forces" briefing as soon as possible after arrival, and every other year thereafter.

8. Policies and Procedures. Persons granted access to SCI, or other sensitive information, incur a special security obligation, and with the exception of official travel, are discouraged from travelling to countries deemed hazardous by the state department or this command. SCI-Indoctrinated and other travellers must be alerted to the risks associated with hazardous travel. Failure to comply with the following provision may result in the withdrawal of access to SCI or classified national defense information, and may be con-

05 FEB 1996

sidered in determining whether future access is warranted.

a. Official Travel. Class I and II Personnel who plan travel to, through, or within countries deemed hazardous shall:

(1) In advance, submit an itinerary to their designated representative.

(2) Receive a Defensive Security Briefing.

(3) Report efforts by any individual, regardless of nationality, to obtain illegal or unauthorized access to classified or sensitive unclassified information. Also any suspected attempts to place cleared individuals in compromising situations, or any contract which suggest possible attempts at exploitation by intelligence services of another country, will be reported. Do not report contacts over non-secure telephone lines.

(a) If possible, while traveling, report unusual incidents to the nearest U.S. Consulate, Attache, Embassy Regional Security Officer, or Post Duty Officer.

(b) Upon return to your duty station, report the unusual incident to the nearest Counterintelligence

office of record. At HQ USEUCOM, this is either the local USAF Office of Special Investigations (OSI), if a member of the USAF, or the 527th USA Military Intelligence Battalion, for other service members, civilians and contractors.

b. Unofficial Travel.

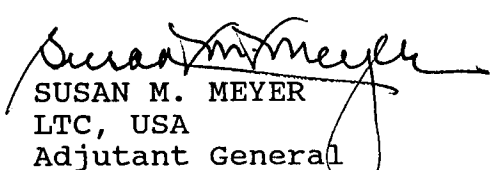
(1) Class I Personnel who plan to travel to, through, or within countries deemed hazardous shall comply with all the aforementioned requirements for official travel.

(2) Class II Personnel are required to comply only with the provisions of paragraph 8.a.(3) above. However, those Class II personnel having SIOP-ESI access must comply with all provisions of paragraph 8.a above.

c. Frequent Official Travel. Class I and II Personnel performing official travel on a continuous basis to hazardous areas may, rather than submitting multiple itineraries, submit a Memorandum For Record stating the location and the anticipated frequency of the travel. This memorandum will be submitted to the designated representative. In lieu of a briefing for each projected travel, the designated representative will arrange a Defensive Security Briefing at least semi-annually.

FOR THE COMMANDER IN CHIEF:

OFFICIAL:


SUSAN M. MEYER
LTC, USA
Adjutant General

RICHARD F. KELLER
Lieutenant General, USA
Chief of Staff

DISTRIBUTION:

P

Appendix A - HQ USEUCOM Form 25-11A-R, 1 Aug 95
Appendix B - HQ USEUCOM Form 25-11B-R, 1 Aug 95
Appendix C - Sample of MFR for Frequent Hazardous Travel
Appendix D - Defensive Security Briefing

CERTIFICATE OF BRIEFING/REQUEST FOR APPROVAL OF TRAVEL FOR CLASS I PERSONNEL

SECTION I - BASIC REQUEST/ITINERARY			
TO: ECJ2-SSO, Personnel Security Office	FROM:	DATE:	
Grade and Name (Last, First & MI)	SSAN	Office Symbol	Duty Phone:

CITY/COUNTRY TO BE VISITED	ARR DATE	DEP DATE	MODE OF TRAVEL

Organization Arranging Tour:	Signature of Requester
------------------------------	------------------------

SECTION II - BRIEFING CERTIFICATE		
<p>CERTIFICATION: I CERTIFY THAT I HAVE RECEIVED A DEFENSIVE SECURITY BRIEFING RELATIVE TO TRAVEL IN COUNTRY(IES) LISTED IN SECTION I.</p>		
Signature of requester	Signature of Briefing Officer	Date

SECTION III - SSO	
APPROVAL _____	DISAPPROVAL _____
<p>COMMENTS:</p> 	
SIGNATURE OF SPECIAL SECURITY OFFICER	

05 FEB 1996

CERTIFICATE OF BRIEFING FOR CLASS II PERSONNEL

SECTION I - BASIC REQUEST/ITINERARY			
TO: EUCOM Collateral Security Office	FROM:	DATE:	
Grade and Name (Last, First & MI)	SSAN	Office Symbol	Duty Phone:

CITY/COUNTRY TO BE VISITED	ARR DATE	DEP DATE	MODE OF TRAVEL

Organization Arranging Tour:	Signature of Requester
------------------------------	------------------------

SECTION II - BRIEFING CERTIFICATE		
CERTIFICATION: I CERTIFY THAT I HAVE RECEIVED A DEFENSIVE SECURITY BRIEFING RELATIVE TO TRAVEL IN COUNTRY(IES) LISTED IN SECTION I.		
Signature of requester	Signature of Briefing Officer	Date

SECTION III - SECURITY
COMMENTS:
SIGNATURE OF SECURITY OFFICER

05 FEB 1996

Sample Memorandum for Record

ECJ3

30-June 1995

MEMORANDUM FOR RECORD

SUBJECT: Frequent Travel into Hazardous Countries ()

1. (U) Missions requirements will make it necessary to travel to Sofia, Bulgaria on a quarterly basis. Travel into the country will be by military air. Ground transportation will be provided through the U.S. Consulate.

2. (U) I received a Defensive Security Briefing on 29 June 1995 by the Directorate Security Officer.

JOHN J. SMITH
Lt Col, USAF
Director of Intelligence

05 FEB 1996

DEFENSIVE SECURITY BRIEFING

C-1. INTRODUCTION. Persons granted access to SCI or classified information incur a special security obligation and should be aware of possible risks of foreign travel. There are certain areas where travel by knowledgeable individuals is considered hazardous. However, because of operational and other unique considerations, travel into these areas may be necessary. The following information is a general purpose travel briefing.

C-2. PURPOSE. U.S. military and government, civilian and defense contractor personnel are considered prime targets of Foreign Intelligence Service (FIS) agents and terrorists groups. The purpose of this briefing is to acquaint you with the risks involved in traveling to foreign countries and to furnish you guidance which may enable you to minimize those risks.

C-3. BACKGROUND. Many foreign countries offer interesting travel brochures, special rates, and other inducements through U.S. branches of their travel bureaus in efforts to attract the growing number of Americans traveling abroad. Past cases reveal that U.S. personnel performing such travel may be subject to surveillance and collection operations by the various foreign intelligence services. Travelers are also subject to terrorism or other acts of violence either by design or by circumstance.

C-4. FOREIGN INTELLIGENCE SERVICES (FIS).

a. Many foreign countries actively engage in the collection of intelligence information. There is no such thing as a "friendly" FIS. The main objective of an FIS is the wholesale collection of data. The most prized type of intelligence data is exploitable science and technology data, followed by the classified government document, but unclassified material, even material which appears to be trivial, can also be of inestimable value. Potentially, the most valuable source of information is that acquired through the use of agents or individuals recruited by an FIS. A Foreign Intelligence Service may gather their information through several different techniques. Probably the greatest achievement an intelligence organization can have is the placement or recruitment of an agent directly in a sensitive position in a national defense or intelligence element of an opposing government.

(1) FIS agents gain their information wherever, whenever, and from whomever they can by employing various tactics to enlist target employees. They may use a seemingly guileless approach, befriending targets, treating them to gifts or money,

wining and dining them. Most FIS believe Americans are hopeless materialists and can be swayed easily by appeals to their greed.

(2) In another maneuver, a FIS agent misrepresents himself as a citizen of a country friendly to the United States. Thus, a targeted American may be duped into handing over sensitive information by being led to believe he is aiding an ally to the United States. In a variation of this tactic, a FIS poses as a representative of a noncommunist country towards which a targeted American is particularly sympathetic. Also, if a FIS believes an individual has communist or similar sympathies, he may make an appeal for information based on ideology. A "pitch" for information may also be geared to take advantage of an American's desire for international harmony and world peace.

(3) Another favored appeal exploits the American belief in freedom of speech and the free exchange of information. For example, a FIS, in the role of scientist, may tell an American scientist that science has no political boundaries. Therefore, in the interest of science, the American is encouraged to share his knowledge with a fellow "member" or the international scientific community.

(4) FIS also use aggressive means in their ceaseless quest for strategic information. To such people, espionage is a business. If they feel coercion and blackmail will serve their purpose, they will not hesitate to employ those methods. As you travel, do not place yourself in a compromising position by engaging in aberrant or promiscuous sexual behavior, black marketing, violating local laws, or by photographing or straying into restricted areas. Many FIS keep travelers under constant surveillance by using agents, video/photographic surveillance, and bugging devices in hotel rooms, bars, restaurants, lounges, and telephones. Such methods may provide them the material to entrap an unwary traveler.

(5) Harassment and provocation are other tools which may be employed by FIS. Travelers may be placed in unusual situations which may cause an incident or elicit a response which would entangle or compromise an individual.

C-5. TERRORIST/CRIMINAL/MOB VIOLENCE.

a. Terrorism. Terrorists have a different objective than a FIS. They are interested in the sensationalism that can be derived from the compromise, embarrassment, interrogation, kidnapping, or death of a U.S. citizen. A terrorist group must know the who, where, when and how to target a specific individual. Therefore, maintaining a low profile and not drawing undue attention to one's affiliation with the U.S. government is essential. Even though an individual may not be targeted for terrorism, and individual can still become a victim of terrorism.

Being at the wrong place at the wrong time may be unavoidable, but the risk of being a chance victim of terrorism can still be reduced.

b. Criminal/Mob Violence. No matter where anyone travels, criminal elements (thieves, muggers, etc.) are present. The foreign traveler is disadvantaged being in an unfamiliar place ignorant of local laws and unable to freely communicate because of a language barrier. In unstable political areas or where the United States is unwelcome, the presence of a U. S. citizen may be enough provocation to cause an incident or become a victim of mob violence. Any minor incident or breach of law or custom involving a U.S. citizen can be blown vastly out of proportion creating a much larger incident.

C-6. TRAVEL GUIDANCE.

A. Personal Concerns. Individuals traveling in hazardous areas should heed the following guidance to avoid possible security or personal problems.

(1) Do not make any reference to your military duties, affiliation with this command or the U.S. Department of Defense.

(2) Advise the U.S. Defense Attache Office (DAO) in each host country of your complete itinerary. Record the address and telephone number of the U.S. Embassy or Consulate in each host or major city in which a visit is planned. Keep your passport on your person at all times and memorize your passport number. Clear wallet and other personal belongings of business cards, notes, or other written material (phone numbers) which might link you to military activities or sensitive plans at your work place.

(3) The Department of State, Consular Affairs provides current, country-specific threat information. Dial (202) 647-5225 for recorded travel information; (202) 647-9225 to access the Consular Affairs bulletin board; or (202) 647-3000 to access the Bureau's automated facsimile system. The system offers consular information sheets, travel warnings, public announcements, tips for travelers brochures, visa bulletins, and other consular information.

B. Hotel concerns.

(1) Do not advertise that you are out of your room. Put the "do not disturb" sign on the doorknob and keep the TV on. Don't leave your room key at the front desk when you depart for the day.

(2) Do not stay above the sixth floor. Many foreign fire companies do not have ladders that go beyond this floor.

105 FEB 1996

The third floor is the best choice. Occupants of rooms lower than the third floor are subject to a higher degree of burglaries or robberies by people entering from the street.

C. Airport/customs concerns.

(1) Be careful to make an accurate and complete declaration of money (including travelers checks) and all valuable (including cameras and jewelry whether worn or carried) on entering the country. It is imperative to retain a copy of this declaration until departure. Use only authorized banks and currency exchanges.

(2) Do not linger in the airport ticketing area after checking in. This is the most vulnerable section of the airport and has been the repeated target for terrorist groups. Proceed to the security area as soon as possible.

D. General Comments.

(1) Be cautious of sexual overtures from anyone. Aside from the potential health hazards, prostitutes are often the decoys who steer individuals into becoming a victim of other crimes, such as robbery and extortion. From a counter intelligence perspective, offers of sexual companionship have historically been a method used by the FIS in an attempt to compromise military members, government employees and government contractors.

(2) Do not attempt to propagandize or engage in political arguments. Many foreign nationals are curious about the U.S., and are genuinely interested in talking to Americans. Their questions are best answered in an objective forthright manner without drawing unfavorable comparisons with the country visited.

(3) Stay with your group or at least some members thereof. If it is necessary to become separated from the group, ensure someone is aware of your whereabouts.

(4) Be careful about accepting invitations. Do not overindulge in drinking or engage in promiscuous activities. Audio (listening) devices and hidden photographic cameras are often planted in rooms.

(5) Do not accept letters, personal messages, photographs, packages or other material to be carried openly or smuggled in or out of the country.

(6) You will almost certainly not, repeat not, be under individual surveillance during your visit. However, if you suspect you are being watched, resist any temptation to "play

games" with what may seem to be clumsy attempts to keep an eye on you. Do not attempt to lose real or imagined surveillance by taking evasive maneuvers, searching your room for listening devices, or attempting to play tricks on such devices if you have ascertained their presence. This sort of action only serves to arouse suspicion and may result in increased foreign security attention and possibly harassment.

(7) Do behave in a natural manner, use good judgement and enjoy your trip.

(8) Maintain a low profile: Blend in with the local populace by wearing suitable attire (Do not over or under dress). Be sensitive to local customs and laws. Travel in pairs or small groups of no more than four people. Use rental rather than official cars if possible. Do not flaunt yourself as an American or attach an "air of importance" to yourself. Avoid being aggressive to the native population. Ensure your itinerary is not publicized, but given to those who have a need-to-know.

(9) Never pick up souvenirs, statutes or artifacts just because they appear to be lying around or unclaimed. Purchase such items in approved shops only, making certain that a receipt is provided for each purchase. Do not sign any receipts for money or services unless first assured of and furnished an on-the-spot copy which clearly identifies and itemizes the nature of the transaction.

(10) Do not make or write any statements which might be exploited for propaganda purposes. Do not sign any petitions, however innocent they may appear.

(11) Do not photograph any military personnel, equipment, installation, defense plant or other military or restricted area. Also, refrain from photographing slum areas, ghettos, or under privileged persons in the host country. It is good policy not to photograph airports and train yards as this is specifically forbidden in many countries.

(12) As a precaution, be aware that clothing may be tagged with invisible dyes and/or radioactive materials. This can be done at a dry cleaning establishment or in your room. If a letter were placed in the tagged pocket and later mailed, it could be retrieved and traced to you. You should be careful about what you write and to whom you write, as mail and telegrams may be censored.

(13) In writing letters, use your own stationery and not that given to you by any local hotel. Also, purchase stamps at a post office or embassy outlet. Stamps obtained at a hotel or other source can be tagged with invisible inks or radioactive tracers. Assume that letters will be opened and read. If

05 FEB 1996

necessary to write about confidential or sensitive matters, use appropriate channels of the U.S. Embassy or Consulate.

E. If detained by the local authorities, remember, tourists generally have nothing to worry about so long as they follow the local rules, and use good judgement. However, occasionally individuals do encounter trouble with authorities, either by mistake, or as the result of some injurious action. Should this occur, most important things to remember are:

a. Insist on being put in contact with the American Consulate at once. If the authorities stall or attempt to intimidate you, refuse to make any statement until this has been done. Experience shows that if an individual cannot be intimidated by vague or implied threats, the detainer will usually back down if the individual has not, in fact, done anything wrong.

b. Under no circumstances sign any document until you have had the opportunity to meet with a U.S. Official.

c. Remain calm, but assertive. Do not antagonize those who detain you, but continue to insist on your right to speak with a representative of the U.S. Government.

F. In the event you are taken hostage in a terrorist situation:

a. Do not physically resist, but passively cooperate with captors.

b. Prepare yourself mentally for a long period of hostage negotiations.

c. Remember that although negotiations are usually lengthy, virtually all hostages are released unharmed.

d. Attempt to establish personal rapport with your captors, while at the same time maintaining your dignity.

e. Do not become involved in controversial discussions with the terrorists.

f. If you observe a rescue party approaching, lie on the floor with your hands covering your head. Do not move until instructed to do so by members of the rescue team.

G. If U.S. military or government civilian personnel should happen to be aboard an aircraft which has been hijacked:

a. If in uniform,

105 FEB 1996

(1) Be as unobtrusive as possible.

(2) Do not attempt to take charge, demand privileges of rank, or to openly advise other passengers as to their conduct.

(3) If asked for identification, show only passport (tourist if possible).

b. If in civilian clothing, do not offer to make known a U.S. military or government affiliation unless forced to do so. Most persons previously placed in such a situation have been requested only to show some reasonable identification (driver's license, passport, credit cards, etc.)

C-7. REPORTING PROCEDURES. Any suspected approach made to you during your travel should be reported as outlined in SD 25-3, paragraph 8.a.(b).